Australian Government

Office of the Australian Information Commissioner

Guide to securing personal information

'Reasonable steps' to protect personal information

January 2015

Contents

Introduction

This 'Guide to securing personal information' (Guide) provides guidance on the reasonable steps entities are required to take under the *Privacy Act 1988* (Cth) (Privacy Act) to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure. It also includes guidance on the reasonable steps entities are required to take to destroy or de-identify personal information that they hold once it is no longer needed (unless an exception applies).

This guide is intended for use by entities covered by the Privacy Act, including organisations, agencies, credit reporting bodies (CRBs), credit providers and tax file number recipients.[1] However, this guide may also be relevant to organisations not subject to the Privacy Act as a model for better personal information security practice.

This guide is not legally binding. However, the Office of the Australian Information Commissioner (OAIC) will refer to this guide when undertaking its Privacy Act functions, including when investigating whether an entity has complied with its personal information security obligations (s 40) or when undertaking an assessment (s 33C). Information on when and how we might exercise our regulatory powers is available in the OAIC's *Privacy Regulatory Action Policy*.

Entities subject to the Privacy Act should read this guide in conjunction with the *Australian Privacy Principles guidelines* (APP guidelines). The APP guidelines outline the mandatory requirements of the Australian Privacy Principles (APPs), how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the Privacy Act.

The introductory sections of this guide include a discussion of what is personal information security, why you should have it, and how you should protect personal information through the stages of its lifecycle. Part A discusses five general circumstances that affect what steps an entity should take to protect personal information. Under nine broad topics, Part B outlines examples of key steps and strategies you should consider taking to protect personal information including a number of questions you should ask yourself when considering or implementing these steps or strategies.

This guide assumes some knowledge of privacy and security concepts. Additional information and resources is available in Appendix B.

The Privacy Act, the APPs, and other obligations

The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government (and Norfolk Island) agencies (APP entities).

[1] For more information on the jurisdiction of the Privacy Act, see our 'Who is covered by privacy' webpage. We have used the term 'entity' throughout this guide to refer to all agencies and organisations subject to one or more of the provisions of the Privacy Act.

APP 11 requires APP entities to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information.[2]

Specifically, APP 11.1 states that an APP entity that holds personal information must take reasonable steps to protect the information from **misuse**, **interference** and **loss**, as well as **unauthorised access**, **modification** or **disclosure.**[3]

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[4] This requirement does not apply where the personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.[5]

An entity 'holds' personal information 'if the entity has possession or control of a record that contains the personal information'.[6] The term 'holds' extends beyond physical possession to include a record that an entity has the right or power to deal with. For example, an entity that outsources the storage of personal information to a third party, but retains the right to deal with that information, including to access and amend it, 'holds' that personal information.[7]

When considering the security of personal information you also need to be mindful of other obligations under the Privacy Act, such as your obligations under APP 8 (Cross-border disclosure of personal information) and APP 12 (Access to personal information).

Other obligations

All entities will also need to be aware of relevant legislation (other than the APPs) that impose other obligations in relation to personal information security.

If you are a credit reporting body or credit provider covered by Part IIIA of the Privacy Act and the registered CR code;[8] a tax file number recipient covered by the *Tax File Number Guidelines 2011*; or a health care provider covered by the *Personally Controlled Electronic Health Records Act 2012* or the *Healthcare Identifiers Act 2010* you may have additional personal information security obligations.

---

[2] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, p 86.

[3] The six terms listed in APP 11, 'misuse', 'interference', 'loss', 'unauthorised access', 'unauthorised modification' and 'unauthorised disclosure', are not defined in the Privacy Act. See Chapter 11 of the APP guidelines for further guidance on the meaning of these terms.

[4] APP 4.3 also requires the destruction or de-identification of unsolicited personal information received by an organisation in certain circumstances.

[5] For more information on destroying or de-identifying personal information see Chapter 11 of the APP guidelines.

[6] See s 6(1) of the Privacy Act.

[7] See APP guidelines Chapter B: Key concepts.

[8] See ss 20Q and 21S of the Privacy Act and cl. 15 of the registered CR code. The provisions in Part IIIA make it clear whether the obligations in Part IIIA replace relevant APPs or apply in addition to relevant APPs. For example, s 21S states that if a credit provider is an APP entity, APP 11 does not apply to them in relation to credit eligibility information.

Under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), Australian Government agencies must also act in a way that is not inconsistent with the policies of the Australian Government.[9] From the security perspective these policies include the Attorney-General's Department's *Protective Security Policy Framework* and the Australian Signals Directorate's *Australian Government Information Security Manual*. These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government.

Other information security resources

The advice provided in this guide is not intended to be exhaustive and it does not seek to replace any existing government or industry resources regarding information security. Compliance with these resources may be a relevant consideration in meeting the Privacy Act's requirements for personal information security.

Resources related to personal information security are widely available and entities should be aware of any relevant government, industry or technology specific standards, guidance, frameworks or obligations and incorporate these into their information security practices. A list of additional resources is at Appendix B.

[9] Under s 21 of the PGPA Act the accountable authority of a non-corporate Commonwealth entity must govern the entity in accordance with paragraph 15(1)(a) in a way that is not inconsistent with the policies of the Australian Government. Paragraph 15(1)(a) is about promoting the proper use and management of public resources for which the accountable authority is responsible.

What is personal information security?

Section 6 of the Privacy Act defines 'personal information' as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable.[10] This might include a person's name and address, medical records, bank account details, photos, videos and even information about what an individual likes, their opinions and where they work.

An important subset of personal information in the Privacy Act is 'sensitive information.' Sensitive information is defined in the glossary, and includes health information.[11] The Privacy Act generally affords a higher level of privacy protection to sensitive information than to other personal information.

Whether information constitutes personal information under the Privacy Act will depend on whether an individual can be identified or is 'reasonably identifiable' in the particular circumstances.

Some information may not be personal information when considered on its own. However, when combined with other information held or available to you, it may become 'personal information'. These pieces of information may be collected by, or become available to, you at different times. Whether an individual is 'reasonably identifiable' from that information will depend on a range of factors, including the time and cost that would be involved in re-identifying them.

It is essential that you are able to recognise the dynamic nature of information, and that information can become personal information sometime after you have collected it. You should be fully aware of the personal information you handle, where it is kept and the risks associated with that information. If it is unclear whether an individual is 'reasonably identifiable' you should err on the side of caution and treat the information as personal information.

Personal information security

'Information security' involves all measures used to protect any information generated by an entity or individual, that is not intended to be made publicly available, from compromise, loss of integrity or unavailability.[12] This can include personal information, security classified information and commercially confidential information.

'Personal information security' is the main focus of this guide and specifically relates to entities taking reasonable steps to protect personal information (including sensitive information) from misuse, interference and loss, as well as unauthorised access,

[10] The full definition of 'Personal information' is set out in the Glossary section.

[11] For more detail on the definition of 'personal information' and 'sensitive information' see the APP guidelines Chapter B: Key concepts.

[12] Australian Signals Directorate, *Australian Government Information Security Manual,* Controls manual, Glossary of Terms – definition of information security, p.314.

modification or disclosure. This will include consideration of matters before you collect personal information, including whether you should collect it at all.

Why is it important?

Personal information security is about more than just ensuring compliance with the requirements of the Privacy Act. If you mishandle the personal information of your customers, it can cause a financial or reputational loss to the customer. In turn, this can also lead to a loss of trust and considerable harm to your reputation. A significant breach may result in a loss of customers or business partners and revenue.

If personal information that is essential to your functions or activities is lost or altered, it can have a serious impact on your ability to undertake business as usual.

The benefits of applying personal information security to your business practices can include more efficient processes. It also reduces the risk of privacy breaches and the time and resources involved in addressing any breaches that do occur.[13]

Many of the steps and strategies in this guide will also assist you to take reasonable steps to ensure good handling of other types of information, such as commercially confidential information.

[13] Certain organisations such as the Ponemon Institute (www.ponemon.org) have sought to quantify the cost of data breaches to business. In its 2014 Cost of Data Breach Study: Australia, Ponemon found the average data breach cost to a company to be $2.8m. A copy of the report can be found on the IBM website or on the Computerworld website. Note registration is required to access the report.

The information lifecycle

If you handle personal information, you should consider how you will protect personal information during the stages of its lifecycle.

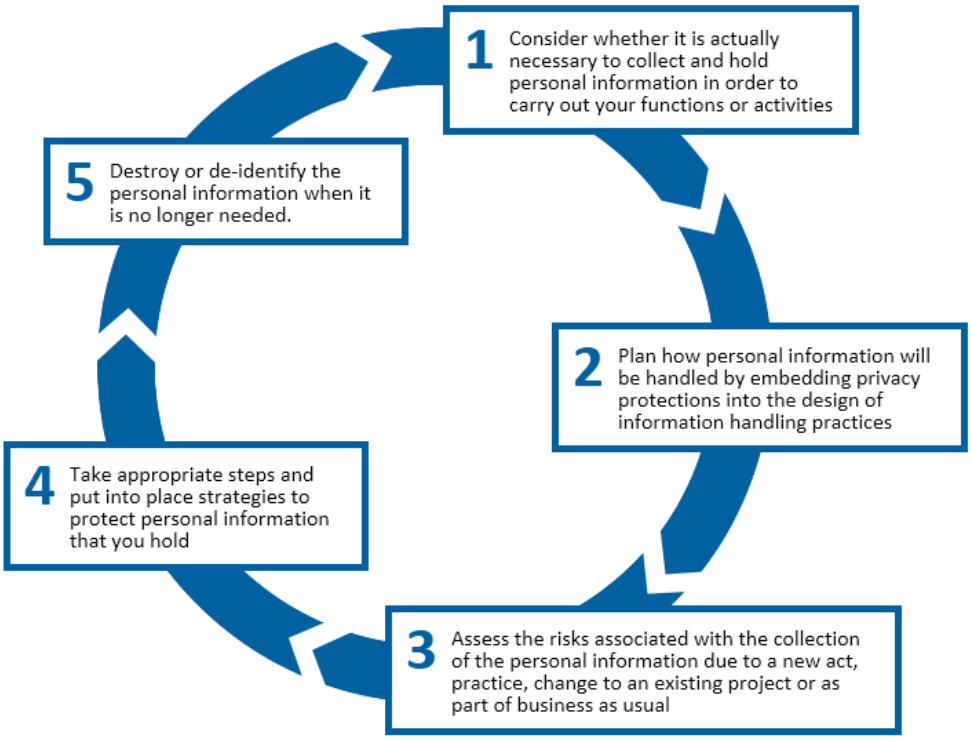
Personal information security throughout the lifecycle involves:

1. considering whether it is actually necessary to collect and hold personal information in order to carry out your functions or activities
2. planning how personal information will be handled by embedding privacy protections into the design of information handling practices
3. assessing the risks associated with the collection of the personal information due to a new act, practice, change to an existing project or as part of business as usual
4. taking appropriate steps and putting into place strategies to protect personal information that you hold
5. destruction or de-identification of the personal information when it is no longer needed.

To effectively protect personal information throughout its lifecycle, you will need to be aware of when and how you are collecting it and when and how you hold it. As noted above, your personal information holdings can be dynamic and change without any necessarily conscious or deliberate action.

Additionally, the lifecycle may include the passing of personal information to a third party for storage, processing or destruction.

The information lifecycle



1. Consider whether to collect personal information

Under APP 3, you should only collect personal information that is reasonably necessary (and for agencies, directly related) to carry out your functions or activities. Over-collection can increase risks for the security of personal information.

Therefore, the first step in managing the security of personal information is to ask whether the collection of personal information is reasonably necessary to carry out your functions or activities.[14] If it is, you should then consider, even if you can collect it, should it be collected? That is, do you really need to collect the personal information or can the collection be minimised?

Personal information that is not collected or is not stored cannot be mishandled.

2. Privacy by design

APP 1 outlines the requirements for APP entities to manage personal information in an open and transparent way. This includes taking reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. The OAIC refers to this as 'Privacy by design'. Privacy should be incorporated into your business planning, staff training, priorities, project objectives and design processes, in line with APP1.

You should design your personal information security measures with the aim to:

- prevent the misuse, interference, loss or unauthorised accessing, modification or disclosure of personal information
- detect privacy breaches promptly
- be ready to respond to potential privacy breaches in a timely and appropriate manner.

You will be better placed to meet your personal information security obligations if you embed them early, including by choosing the appropriate technology and by incorporating measures that are able to evolve to support the changing technology landscape over time. You also need to take into account the rapid development of new and existing technologies and platforms when designing your information security policies and systems.

An important element of 'privacy by design' is to integrate privacy into your risk management strategies (see 'Assessing the risks' below). Robust internal personal information-handling practices, procedures and systems can assist you to embed good personal information handling practices and to respond effectively in the event a privacy breach occurs.

[14] For agencies it can also be collected if it is 'directly related' to its functions or activities.

3. Assessing the risks

Assessing the security risks to personal information is also an important element of 'privacy by design'. You can assess your personal information security risks by conducting a privacy impact assessment (PIA), an information security risk assessment and regular reviews of your personal information security controls. You should use PIAs and information security risk assessments along with regular reviews so that you are aware of the variety of security risks you face, including threats and vulnerabilities, along with the possible impacts before designing and implementing your personal information security framework. They will also assist you in integrating privacy into your risk management strategies.

PIAs

A PIA is a written assessment that identifies the privacy impacts of a proposal and sets out recommendations for managing, minimising or eliminating those impacts. Generally, a PIA should:

- describe the personal information flows in a proposal
- analyse the possible privacy impacts of those flows
- assess the impact the project as a whole may have on the privacy of individuals
- explain how those impacts will be eliminated or minimised.

A PIA, especially one conducted at the early stage of a proposal's development, can assist you to identify any personal information security risks and the reasonable steps that you could take to protect personal information. A PIA can also be seen as an iterative process during the life of any proposal, being updated to take account of changes to the proposal as it evolves.

A detailed guide to conducting PIAs is available from the OAIC website. The OAIC encourages entities to undertake a PIA for any new proposals across all business activities that involve the handling of personal information.[15] The PIA guide includes a threshold assessment to assist you in determining whether it is appropriate for you to undertake a PIA. It will depend on a proposal's size, complexity and scope and the extent to which it involves personal information.

While the PIA guide focuses on undertaking PIAs for new projects, you should also consider applying the same principles across your business generally, including existing business operations, to give a greater understanding of the privacy risks that exist currently. Entities should also consider building the use of PIAs into their risk management processes and plans.

[15] Under s 33D of the Privacy Act, if an agency proposes to engage in an activity or function involving the handling of personal information and if the OAIC considers that the activity or function might have a significant impact on the privacy of individuals, the OAIC may direct the agency to give the OAIC, within a specified period, a PIA about the activity or function.

Information security risk assessments

You may also need to conduct an information security risk assessment (also known as a threat risk assessment) in conjunction with a PIA. An information security risk assessment is generally more specific than a PIA because it involves the identification and evaluation of security risks, including threats and vulnerabilities, and the potential impacts of these risks to information (including personal information) handled by an entity. As with a PIA, an information security risk assessment can be seen as an iterative process and may be undertaken across your business generally.

The findings of a PIA and information security risk assessment should inform the development of your risk management and information security policies, plans and procedures.

Once the risks have been identified, you should then review your information security controls (virtual and physical) to determine if they are adequate in mitigating the risks. Given that processes, information, personnel, applications and infrastructure change regularly, and given the constantly evolving technology and security risk landscape, regular review and monitoring of personal information security controls is crucial.

Risk of human error

Threats to personal information can be internal or external as well as malicious or unintentional. Privacy breaches can arise as a result of human activity or events such as natural disasters. Human error is regularly claimed as the cause of privacy incidents; however entities should assume that human error will occur and design for it.[16] Research has shown that human error can be seen as a trigger rather than a cause of an incident.[17] PIAs, information security risk assessments and regular reviews will enable you to design practices, procedures and systems to deal with the foreseeable risk of human error and minimise its effect.

4. Taking appropriate steps and putting into place strategies to protect personal information

Once your entity has collected and holds personal information, you need to consider what appropriate security measures are required to protect the personal information. This will need to be considered in regards to all of your entity's acts and practices. Part B of this guide sets out examples of key steps and strategies you should consider taking in order to protect the personal information you hold to satisfy your security obligations under the Privacy Act.

[16] See the Own motion investigation report AICmrCN 5. This case illustrates how the failure to put in place adequate policies, procedures and systems to mitigate the risk of human error can result in a data breach. Failures at a number of levels aligned to create circumstances that enabled a breach to occur.

[17] This approach is based on the 'Swiss cheese' or 'cumulative act effect' model of accident causation which is an illustration of how organisational failures at a number of levels can combine to create a situation in which human error can trigger a data breach. This is a model used in risk analysis and risk management originally propounded by Dante Orlandella and James T. Reason in 1990.

5. Destroy or de-identify personal information

Under APP 11.2, APP entities must also take reasonable steps to destroy or de-identify the personal information they hold once it is no longer needed for any purpose for which it may be used or disclosed under the APPs.[18] This requirement does not apply where the personal information is contained in a 'Commonwealth record' or where the entity is required by law or a court/tribunal order to retain the personal information.

Destroying or permanently de-identifying personal information that you no longer need is an important risk mitigation strategy and is discussed in Part B.

[18] APP 4.3 also requires the destruction or de-identification of unsolicited personal information received by an organisation in certain circumstances.

Part A — Circumstances that affect assessment of reasonable steps

What qualifies as reasonable steps to ensure the security of personal information depends on the circumstances, including the following:

- the nature of your entity
- the amount and sensitivity of the personal information held
- the possible adverse consequences for an individual in the case of a breach
- the practical implications of implementing the security measure, including the time and cost involved
- whether a security measure is itself privacy invasive.

These circumstances will also influence the reasonable steps you should take to destroy or de-identify personal information.

The examples of OAIC investigations discussed below are intended to assist an entity to understand our guidance. They reflect a point in time circumstance in relation to the particular organisation.[19] Even slight changes to the facts expressed in the examples may lead to a different result.

Nature of the entity

The size of your entity, its resources, the complexity of its operations and the business model, are all relevant to determining what steps would be reasonable to protect the personal information you hold. For instance, a franchise or a business using outsourcing is likely to provide access to its personal information to third parties (franchisees and contractors). The reasonable steps it takes may be different to those it would take if it did not operate in this manner.

Example 1:

An investigation into a telecommunications company following allegations that customer information had been compromised showed that the company's business model provided access to the company's databases of customer information to dealership employees via a shared store login ID.

Although the use of shared logins and the wide availability of full identity information is an inherent personal information security risk, in this instance the risk was increased by the fact that the entity had less control over information being accessed through dealerships, and no way of tracking or auditing who was accessing the information.

Read the full investigation report for Example 1

[19] The examples of OAIC investigations were undertaken before the commencement of the APPs on 12 March 2014 and therefore refer to the National Privacy Principles (NPPs), specifically NPP 4 (replaced by APP 11). However the examples are still relevant in relation to the circumstances that will affect whether an entity has taken reasonable steps to protect personal information under APP 11.

When you outsource any of your personal information handling to a third party (including to a cloud service provider), and you continue to 'hold' that information, you will still be subject to APP 11. Part B sets out steps to assist you when implementing information handling practices.

Example 2:

The information handling practices of a telecommunications company and its internet service provider (ISP) were considered in an investigation following media reports that a server holding the telecommunications company's customer personal information had been compromised by an external attack.

The investigation found that the telecommunications company and the ISP failed to take reasonable steps to manage and protect personal information held on the compromised server. For example, it was found that the telecommunications company did not have adequate contractual measures in place to protect the personal information held on the compromised server.

Read the full investigation report for Example 2

If you are disclosing to an overseas recipient you may need to take further steps to comply with APP 8, the cross border disclosure principle.[20]

Amount and sensitivity of personal information held

Generally, as the amount and/or sensitivity of personal information that is held increases, so too will the steps that it is reasonable to take to protect it.

The community generally expects that their sensitive information will be given a higher level of protection than non-sensitive information. This expectation is reflected in the increased privacy protections which apply to the handling of sensitive information.

Although it is not defined as sensitive information under the APPs, people often expect that their financial information will be given a high level of protection. The protections in the Privacy Act in relation to credit reporting information and tax file numbers reinforce this.

[20] See APP guidelines, Chapter 8 for further information.

Example 3:

The sensitivity of the information was taken into account in an investigation into a telecommunications company following media allegations that personal information of the company's customers was accessible online, which was confirmed by the company.

The personal information of approximately 15,775 customers was compromised, including full names, addresses and phone numbers, including 1,257 customer accounts with silent numbers. The Commissioner stated that a breach of this type of personal information for the 1,257 customers with silent number was not low risk. Further, the Commissioner noted that different risk levels may require an entity to take different security precautions in order to meet the requirements of the Privacy Act. The Commissioner stated that it was a reasonable step for the company to implement security processes and procedures to address the heightened risk environment.

Read the full investigation report for Example 3

Adverse consequences for an individual

When you are assessing the steps that you will take to protect personal information, you should consider the possible adverse consequences for the individuals concerned if the information is not secured. This may extend to material harm from identity theft or fraud.

The mishandling of some kinds of sensitive information, such as health information that identifies an individual's medical condition, may:

- provide the basis for discrimination or other forms of harm
- lead to humiliation or embarrassment, or undermine an individual's dignity.

The likelihood of harm occurring will be relevant in considering whether it is reasonable to take a particular step.

Example 4:

The necessity of considering the risk of adverse consequences is highlighted by a case where an Australian Government department published statistical data of highly vulnerable people without taking appropriate steps to ensure it was not identifiable.

An investigation found that the department was aware of the privacy risks of embedding personal information in publications, but that their systems and processes failed to adequately address those risks. The likelihood of harm to the individuals affected was a key consideration in assessing whether the department had taken reasonable steps.

Read the full investigation report for Example 4

Practicality of implementation

The practicality of implementing a security measure, including the time and cost involved, will influence the reasonableness of taking that step.

However, you are not excused from taking specific steps to protect information just because it would be inconvenient, time-consuming or costly to do so. Whether these factors make it unreasonable to take particular steps depends on whether the burden is excessive in the specific circumstances.

In deciding whether these factors make a step unreasonable, you should have regard to other circumstances such as the sensitivity of the personal information and the risk to an individual if that information is misused, interfered with, lost, or inappropriately accessed, modified, or disclosed.

Example 5:

An investigation into a medical centre found that there were boxes of unsecured medical records being stored in a garden shed at a site no longer occupied by the medical centre.

The medical centre advised the Commissioner that patient health records were transferred from the locked room inside the former premises to a garden shed at the back of the site (so that renovations for sale of the site could occur). The garden shed door was locked with padlocks.

The Commissioner found that the medical centre did not take reasonable steps to protect the personal information, some of which was also sensitive information. Further, the Commissioner did not consider there to be any circumstances in which it would be reasonable to store health records, or any sensitive information, in a temporary structure such as a garden shed.

Read the full investigation report for Example 5

Privacy invasiveness

It may not be reasonable to implement a security measure if it is itself privacy invasive. For example, requiring users to supply extensive personal information to identify themselves prior to giving access to their records under APP 12 may result in collecting personal information that is unnecessary (contrary to APP 3).[21]

In that instance, you will need to balance what you need to do to prevent disclosure of personal information to the wrong person with the need to ensure that access is given on request.

[21] APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request.

Part B — Steps and strategies which may be reasonable to take

Appropriate security measures for protecting personal information need to be considered in regards to all of your entity's acts and practices. This section outlines examples of key steps and strategies you should consider under the nine broad topics listed below. It includes a number of questions to ask yourself when considering or implementing these steps and strategies.

- Governance, culture and training.
- Internal practices, procedures and systems.
- ICT security.
- Access security.
- Third party providers (including cloud computing).
- Data breaches.
- Physical security.
- Destruction and de-identification.
- Standards.

These steps and strategies are not intended to be prescriptive or exhaustive and it may not be necessary to take all the steps and strategies outlined below. You should also consult relevant standards and guidance on information security including any which are particular to your sector or industry (see 'Standards' and 'Information security resources' below).

The steps and strategies vary in ease of implementation and the impact that they will have on users. What is reasonable in the circumstances may vary between entities, and may change over time, for example, as a result of technological change or if you become aware that security measures that previously protected personal information are no longer adequate.

You should be fully aware of all the personal information you handle, where it is kept and the risks associated with that information before deciding what steps to take. You could undertake robust information asset management by developing and maintaining a list or register which provides a high level description of the types of and location of personal information you handle. This will help ensure that your personal information security measures are comprehensive.

Many of the steps and strategies in this guide may also assist you in protecting other types of information, such as commercially confidential information.

Governance, culture and training

Fostering a privacy and security aware culture

Your privacy and security governance arrangements should include appropriate training, resourcing and management focus to foster a privacy and security aware culture among your staff. Personal information security should be an integrated component of your entire business and not left to the compliance or ICT area alone. The creation of this culture will require the active support of and promotion by, senior management.

Insufficient interest in personal information security from staff, in particular senior management including the board (or equivalent decision making body), can lead to threats to the security of personal information being ignored and not properly attended to. Appropriate training can assist in mitigating these issues and making staff aware of common personal information security threats (see 'Personnel security and training' section below).

If your entity has experienced a significant breach of personal information security, the focus of your senior management should be to look at whether significant cultural changes are needed to improve security in the long term rather than relying on superficial solutions or treating such issues as 'someone else's problem'.

Oversight, accountability and decision-making

You should establish clear procedures for oversight, accountability and lines of authority for decisions regarding personal information security. You could have a body or designated individual/s that are aware of what personal information you hold, where and how it is held and responsible for ensuring that it is held securely. This role could include defining information security measures and implementing and maintaining those measures. This role should be overseen by, and accountable to, your senior management.

- Are privacy and personal information security steps and strategies driven by your senior executives?
- Do the governance arrangements foster a privacy and security aware culture among your staff?
    - Do the governance arrangements promote awareness and compliance with personal information security obligations?
    - What governance arrangements do you have in place?
- Are there clear procedures for oversight, accountability and lines of authority for decisions related to personal information security?
    - Is it clear who is responsible for the overall operational oversight and strategic direction of your information handling projects?
    - Are there distinct areas or persons who have responsibility for security and privacy issues?
        - Are these areas or persons aware of what personal information you hold and where and how it is held?

- If there are several areas or teams responsible for information security and privacy, are there governance arrangements in place to ensure that they work together, creating a focal point for privacy advice and solutions and preventing silos?
- Are regular meetings held at the senior management and operational level to discuss security and privacy issues and incidents?

- Do your change management processes include consideration of the effect of changes on personal information security?
- Do governance arrangements include risk management and business continuity plans?
- Are there ICT governance protocols in place? For example are there persons responsible for the accreditation and approval of personal information security controls to ensure that each control is effective and appropriate?

Personnel security and training

Personal information security includes ensuring your entire staff are aware of their privacy and security obligations (including senior management). Human error can be a contributing cause to data breaches and undermine otherwise robust security practices where the systems have not been designed to deal with it.[22]

It is therefore important that all staff understand the importance of good information handling and security practices. Privacy training may help staff understand their responsibilities and avoid practices that would breach your privacy obligations. Training should take into account new starters, contractors and temporary staff.

- Where appropriate, do staff have appropriate security clearances or undergo security vetting?
- Are staff provided with training on physical and ICT security and the handling of personal information?
  - When is training provided to new starters?
  - Is training also provided to short term staff and contractors?
  - Is refresher training provided to your staff and does this occur on a regular basis?
  - Are your staff informed of your internal practices, procedures and systems which relate to the handling of personal information? (see 'Internal practices, procedures and systems' section below)
  - How are your staff informed of changes to these practices, procedures and systems?
- Is personal information security training of staff considered at the project design stage?

[22] See the Own motion investigation report AICmrCN 5. The case illustrates how the failure to put in place adequate policies, procedures and systems to mitigate the risk of human error can result in a data breach.

- Is there an appropriate amount of training, resourcing and active management support to promote a privacy and security aware culture?
  - Does training emphasise to staff the importance of not accessing personal information or databases unnecessarily?
  - Does training make it clear to staff what would constitute misuse of personal information?
  - Does training cover identity authentication procedures?
  - Does training emphasise to staff the importance of authentication processes not infringing customer/client privacy?
  - Does this training cover recognising and avoiding inadvertent disclosures?
    - When verifying an individual's identity?
    - When publishing files online — are staff trained to identify and remove embedded personal information not intended for public release?
- Does training address the need to avoid weak passphrases and passphrase reuse?
- Are staff reminded on a regular basis of their obligations to handle personal information appropriately?
  - Are there signs in the workplace or alerts on computer systems?
  - Do computer logon screens outline staff privacy and security responsibilities?
- When a staff member moves to a different position, or leaves your organisation or agency, is their access to personal information reviewed or revoked?
- Are staff trained to report privacy issues to the area or persons who have responsibility for security and privacy issues?
- Does training cover recognising and avoiding 'phishing' and 'spear phishing' attacks and 'social engineering'?
- Are staff advised on how to mitigate against unauthorised access if they discuss customers' or clients' personal information over the telephone?
- Are there procedures governing the printing of documents containing personal information?
- Is there a policy that covers information security when staff members work offsite, such as from home, a secondary site office or a temporary office?
  - What standards of physical security are applied to those workspaces, for example, the appropriate storage of physical files?
  - If employees are given remote access to work ICT systems, what measures are in place to secure this access?
  - Who has overall responsibility for the security of personal information at those workspaces?

- Are there clear polices governing the use of end-user mobile devices, including use of staff's own devices (known as 'Bring Your Own Device (BYOD)') and procedures for taking work home?
    - Are there minimum standards for security of end-user mobile devices (such as password protection, encryption)?
    - Are return address labels placed on end-user mobile devices in case of loss?
    - Are staff members educated about the risks of accessing or handling the entity's data on unauthorised/insecure devices, including the risks associated with BYOD practices?
    - If it is necessary for staff to take personal information off the premises, what steps do you take to ensure the security of personal information that is removed?
    - Is confidential business information segregated from personal user information?

Internal practices, procedures and systems

Under APP 1.2, entities are required to take reasonable steps to establish and maintain practices, procedures and systems that will ensure compliance with the APPs and any binding registered APP code.[23]

For the purposes of APP 11, you should document the internal practices, procedures and systems that you use to protect personal information. Your documentation should outline the personal information security measures that are established and maintained against the risks and threats to personal information. These documents should be regularly reviewed and updated to ensure they reflect your current acts and practices.

You could also consider documenting the security choices you have made about your security profile, including the reasons why you have or have not adopted specific personal information security measures.

Internal practices, procedures and systems which relate to personal information security may be addressed in a single policy or in a number of separate policies.[24] Additionally, you should make sure that staff are aware of, and have access to, these policies and are trained regarding their responsibilities (see 'Governance, culture and training' section above).

- Do you have policies which address personal information security matters, such as the physical, ICT and access security and other appropriate personal information handling practices?
    - Did a PIA and an information security risk assessment inform the development of these policies?
    - Are your documented policies easy to understand?

[23] For further information see the APP guidelines, Chapter 1.

[24] Use of the term 'policy' in this section refers to your entity's internal documentation regarding its personal information security profile, not its APP privacy policy which is discussed in APP 1.3-1.6.

- If there are multiple policy documents involved, is it clear how they relate to each other, for example their hierarchy or order of importance?
- Do the policies use language and concepts that are consistent with the Privacy Act?
- Do your policies refer to your obligations under the Privacy Act and other laws to protect personal information? Do they clearly explain how these obligations underpin these policies?
- Are all staff, including short-term staff and contractors, aware of and able to access these policies easily?
- Do these policies reflect your current acts or practices? Are mechanisms in place for ensuring that policies are updated and regularly reviewed?
- Are mechanisms in place to enable staff members to seek clarification or suggest updates?
- How do you ensure compliance with internal policies, for example, are there designated privacy officers and regular reporting to the entity's governance body to ensure this occurs?
- What steps do you take if it becomes evident that staff members are not observing elements of your policies?
- Is there a conflict of interest policy in place that instructs staff members on how to proceed if they handle personal information relating to a person known to them?

ICT security

Effective ICT security requires protecting both your hardware and software from misuse, interference, loss, unauthorised access, modification and disclosure. However, ICT security measures should also ensure that the hardware, software and personal information stored on it remain accessible and useful to authorised users.

It is expected that entities regularly monitor the operation and effectiveness of their ICT security measures to ensure that they remain responsive to changing threats and vulnerabilities and other issues that may impact the security of personal information.

You should be aware of the personal information you hold on your ICT system and where it is located. Your ICT security measures should ensure that all of your systems are secure and that they provide a safe environment for your:

- staff to carry out your business
- customers to interact with your agency or business, for example when they make payments or provide their banking details and/or other personal information.

You need to consider the security of all systems that use or interact with your ICT system. This includes securing your website(s), social media platforms, mobile device applications

(apps)[25] along with Internet connected end-user mobile devices (such as smartphones, tablets and laptops), portable storage devices, desktop terminals, kiosks, as well as Wi-Fi networks, remote access and other aspects of your systems.

ICT security measures help mitigate the risks of internal and external attackers and the damage caused by malicious software such as malware, computer viruses and other harmful programs. These programs can be used to gain unauthorised access to your computer systems in order to disrupt or disable their operation and steal any personal information stored on those systems. ICT security measures can also help mitigate the risks of internal threats.

As well as ICT security against external and internal threats, it is important to consider the possibility of:

- human error (for example, misplacing devices such as laptops and data storage devices, noting that encryption and password protection can mitigate this risk)
- hardware or software malfunctions
- power failure
- system failure caused by natural disasters such as earthquakes, floods, and extreme weather conditions.

Software security

You should consider whether the software you use is sufficiently secure. Errors made during software development can potentially result in privacy breaches.

- Do you regularly review your software security to confirm its continued effectiveness? Is software tested to ensure that there no flaws which can result in privacy breaches?
- Has security software been deployed across all network components (for example on servers and network gateways), not only workstations?
- Are the latest versions of software and applications in use?

Patches can result in a number of extra functions and features that should be assessed for their privacy impacts before they are installed.[26]

- What processes are in place to ensure that patches and security updates to applications and operating systems are installed as they become available?

[25] The OAIC has developed a guide to help mobile device application (app) developers embed better privacy practices in their products and services. The OAIC's *Mobile Privacy: A Better Practice Guide for Mobile APP Developers* is available on the OAIC website.

[26] Patches are software that is used to correct a problem with a software program or a computer system.

Removing or disabling unneeded software, operating system components and functionality from a system reduces its vulnerability to attack, and can make it harder for malware to run or an attacker to gain access.

- Are operating system functions that are not required disabled (for example AutoPlay or remote desktop access)?

There is a risk that content delivered through websites can be used to arbitrarily access system users' files or deliver malicious code. This risk can be reduced by ensuring that software applications and web browsers, including 'add-ons' or 'plug-ins' are up to date.[27] Disabling unused applications may also assist in preventing unauthorised access to a computer system.

- Are applications and web browsers configured for maximum security (eg. plug-ins up to date, unused applications disabled)?
- Are add-ons and plug-ins regularly reviewed and updated?

If you are downloading or using web applications (such as web-based email, wikis, directly updating personal details on databases) or importing data to a system, you should ensure that appropriate security and scanning measures are in place.

- Are all email attachments received from an external source scanned before they are opened?
- Are computer files scanned and checked for abnormalities at workstation level?
- Do you have security measures in relation to web applications?

Encryption

Encryption is important in many circumstances to ensure that information is stored in a form that cannot be easily understood by unauthorised individuals or entities. Encryption methods should be reviewed regularly to ensure they continue to be relevant and effective and are used where necessary. This includes ensuring that the scope of encryption is wide enough so that attackers cannot access another unencrypted copy of your encrypted information.

- What encryption methods do you use? Are they reviewed regularly to ensure they are effective?
- Have you considered whether you should employ encryption of:
    - Databases used to store personal information?
    - Servers?
    - Backups?
    - Information stored in third party cloud servers?
    - Internal network communications, such as email or file shares?

[27] Add-ons and plug-ins are software that add specific functions to a browser

  - End-user mobile devices, such as smartphones, tablets and laptops, including BYOD?
  - Portable storage devices?
  - Data in transit, for example data transferred over the Internet?
- How are decryption keys managed?[28]
- Do you enable encrypted communications on your website (for example, for making payments)?
- Is there another unencrypted copy of your encrypted data?

Network security

You need to have appropriate security controls in place to protect your network. The security controls that are appropriate will depend on the circumstances.

Intrusion prevention and detection systems can be an effective way of identifying and responding to known attack profiles. This may include using firewalls, which control the incoming and outgoing network traffic, and software applications, such as filtering, that monitor network or system activities for malicious activities, anomalous behaviour, or policy violations.

- Do you employ and maintain an intrusion prevention and detection system and regularly analyse event logs?
- What sorts of firewalls are employed and are they appropriately configured?
- Is both incoming and outgoing web traffic filtered?
- How do you monitor and detect unauthorised downloading, transferring or theft of bulk data, for example through the use of personal storage devices?

Spammers may use spoofed email to try to bypass filters and make it appear as though email comes from a legitimate source.[29] Such emails may ask the recipient to provide their own or other individuals' personal information.

- Do you have systems in place to protect your email systems from malware, spam and spoofing, including blocking spoofed email?
- Do you employ email validation and authentication systems, for example the Sender Policy Framework[30] and Domain Keys?[31]

[28] Decryption is the process of converting encrypted data back into its original form, so it can be understood. In order to easily recover the contents of encrypted information, the correct decryption key is required.

[29] Spoofed email is email in which parts of the email header are altered so that it appears to have come from a different source.

[30] Sender Policy Framework is an email validation system designed to detect email spoofing by allowing receiving mail exchangers to check that incoming mail from a domain is being sent from a host authorised by that domain's administrators.

[31] DomainKeys is an email authentication system designed to verify the domain of an email sender and that the email message was not modified in transit.

Separating an entity's network into multiple functional segments makes it difficult for an intruder to propagate inside the network. Proper network segmentation assists in the creation and maintenance of network access control lists. Segmentation can also allow for different security measures to be applied to different types of information depending on its sensitivity and the risks associated with it.

- Is the network segmented and segregated into security zones?
- Are different security measures applied to different security zones, depending on the type of information in that zone and the risks associated with it?
- Does the information with the highest risk have the highest level of protection applied?
- What steps have been taken to ensure that this information is not inadvertently taken outside of the secured environment?
- Are downloaded files quarantined from the network until it is established that they are safe (opened in a segregated testing environment such as a sandbox)?

Whitelisting and blacklisting

Whitelisting and blacklisting are ways of controlling the content, applications or entities that are allowed to run on or access a device or network.[32]

Both can prevent potentially harmful material from accessing your system. Whitelisting may offer greater protection than blacklisting as it is not dependent on identifying the material to be blocked. However, a drawback is that it can also block harmless content that is not whitelisted. Reputation-based lists used for blacklisting need to be maintained and updated to be effective due to the rapid pace with which malicious sites come and go.

- Is whitelisting of applications, email attachments and web domains and IP addresses employed?
- If not, has blacklisting of applications, email attachments and web domains and IP addresses been used instead?
    - If so, what steps are in place to ensure the blacklist remains relevant, up to date and complete? For example, is the blacklist automatically updated from time to time?

Testing

Testing of ICT systems should occur during their development, transition to operations and regularly once they are operational. Depending on the situation, you may wish to consider penetration (or vulnerability) testing to discover security weaknesses, or configuration reviews, to test whether networks are operating towards a certain standard.

[32] Whitelisting is permissive — it is a list of the content, applications or entities that are allowed. Blacklisting is prohibitive — it is a list of the content, applications or entities that are not allowed.

You need to consider how to scope your testing — remember that testing only discrete elements of your ICT system may miss systemic issues.

- How often is testing conducted?
- Does it cover all aspects of the system?
- Who is responsible for conducting testing (eg. internal, independent)?
- How is test data handled?
- Is actual personal information or dummy data used for testing? If actual personal information is used:
  - has a PIA and information security risk assessment been undertaken to assess the personal information flows caused by the testing?[33]
  - do your internal practices, procedures and systems reflect the use of personal information for testing?
- If testing identifies weaknesses, how is this reported and addressed?

Backing up

To prevent personal information you hold from being lost, you should make copies of important files and store them on a physical device or online using a cloud-based storage solution.

- Are backups set up to run frequently?
- Is all essential information included in backups?
- How far back is data recoverable?
- Do you have a data retention policy which reflects APP 11.2?
- Do you review your backups to check that personal information that is no longer needed is:
  - destroyed or de-identified
  - if contained in a Commonwealth record, handled in accordance with the Archives Act
  - if required by law or a court/tribunal, is retained? (see 'Destruction or de-identification of personal information' section below)
- Are backups regularly tested to see if the data is recoverable?
- Are physical devices used to store your backup files kept in a secure location?

[33] An example of a 'use' that an individual may be taken to reasonably expect is use for the secondary purpose of a normal internal business practice, such as auditing, business planning, billing or de-identifying personal information. The OAIC generally considers that the use of personal information to test ICT security systems may be a normal internal business practice in limited circumstances, such as where it is unreasonable or impracticable to use de-identified or dummy data (subject to the exception in APP 6.2(a)). For further information see APP guidelines, Chapter 6, paragraph 6.22.

- Are backups stored remotely to protect from natural disasters?

Email security

Email is not a secure form of communication and you should develop procedures to manage the transmission of personal information via email.

- Do you avoid sending certain types of personal information via unsecured email (for example sensitive information)?
- Do you use secure methods for communicating information, such as a secure website or to a secure online mailbox?
- Do you use secure messaging where appropriate and available?
- Do you obtain a recipient's consent to send their own personal information to them via email?
- Do you validate the email address with the recipient before sending the unencrypted email to reduce the chance of unauthorised disclosure to a party who is not the intended recipient?
- Do you ensure that accurate records are kept regarding when external emails are sent and received?
- Do you only send sensitive information or large amounts of non-sensitive personal information by email as an encrypted or password protected attachment?

Access security

Access security and monitoring controls help you protect against internal and external risks by ensuring that personal information is only accessed by authorised persons.

'Unauthorised access' is a separate concept from 'disclosure', as an entity is not taken to have disclosed personal information under APP 6 (Use and disclosure) where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. However, the entity may breach its security obligations under APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access.

Trusted insider risk

You need to guard against internal threats such as unauthorised access or misuse of personal information by your staff, including contractors (the trusted insider risk). Trusted insider breaches can occur when staff mishandle personal information while carrying out their normal duties. These actions are often motivated by personal advantage, for example insiders accessing personal information for financial gain.

To minimise this risk you should, when possible, limit internal access to personal information to those who require access to do their job (ie provide access on a 'need to know' basis). Limiting such access is an important personal information security mechanism.

If someone is transacting with you using a pseudonym, you could also consider further restricting access to personal information that is linked to that person to protect the pseudonym.[34]

- Do you limit access to personal information to those staff necessary to enable your entity to carry out its functions and activities?
- Is the number of users with administrative privileges limited to staff requiring those privileges?
- Is access revoked promptly when no longer required?
- Have you considered restricting access to personal information when a customer/client is using a pseudonym?
- Have you considered physically disabling USB or other external port access to devices or disabling internal cd/dvd writers in devices?
- Have you considered employing remote wiping software to allow for the deletion of personal information stored on end-user devices which have been lost or stolen?

Identity management and authentication

You should have processes in place to identify individuals accessing your systems and control their access by associating user rights and restrictions with their identity. This will ensure that only authorised persons can access your systems.

Authentication is a key part of this process and is often managed by providing one of three factors— something one knows (such as a password or code), something one has (a physical token, such as a bank card, security pass, or a mobile phone to receive SMS confirmation), or something one is (biometric information such as a fingerprint). 'Multi-factor authentication' requires at least two factors.

Appropriate authentication can be used to limit a person's access both to the system or network and also to the information contained within it. It can also assist in mitigating security risks such as 'social engineering'[35] (including 'phishing' and 'spear phishing'[36]).[37]

- What factors do you use for authentication?
- Is multi-factor authentication employed in circumstances that may pose a higher security risk (such as remotely accessing a system or where they are accessing sensitive/restricted personal information)?

[34] APP 2 covers issues related to anonymity and pseudonymity.

[35] 'Social engineering' is a term used to describe manipulating individuals into revealing confidential information or performing actions such as granting access to systems.

[36] 'Phishing' typically involves sending an email that appears to come from a legitimate organisation and attempts to trick the recipient into supplying personal information. 'Spear phishing' is a personalised attack utilising personally relevant information to attempt to appear legitimate to a particular user.

[37] According to Verizon's *2014 Data Breach Investigations Report*, p.10 phishing was the third most commonly seen threat action in 2013, see www.verizonenterprise.com/DBIR/2014/.

- Have technical solutions which block or mitigate the effects of phishing, spear-phishing and social-engineering attacks been applied (where appropriate)?

Access to non-public content on web servers

If you host content that is not intended for public release (non-public content) on your web servers, you should consider storing this content elsewhere or restrict access to this information to authorised and authenticated users only. This ensures that non-public content will not be accessed by unauthorised third parties, including search robots[38] such as GoogleBot.[39] In conjunction with authentication, you should also disable directory browsing when configuring web servers.[40]

- Are there clear policies and procedures in place governing the identification and removal of embedded personal information from files before they are published online where the information is not intended for public release?

If you store non-public content on your web servers:

- Do you have access controls in place?
- Can the information be stored on a separate system which is not publicly accessible?
- Have you disabled directory browsing on your web servers?
- Are web servers configured to request search robots such as GoogleBot (via the robots.txt.file)[41] not to index, archive or cache files containing personal information?
- Do you regularly review and monitor your web servers to ensure that:
    - files containing non-public content are not vulnerable to being accessed by unauthorised persons?
    - you are aware of unusual or anomalous traffic on the website? (see 'Audit logs, audit trails and monitoring access' section below).

[38] Search robots or bots are software programs which run automated repetitive tasks over the Internet. They are most commonly used by web search engines and other sites for 'Web crawling' or 'Web spidering'. This involves a search engine using bots to discover new and updated pages which are then added to the search engine's index of Web content.

[39] GoogleBot is Google's web crawling bot.

[40] Directory browsing gives permission to users to view a listing of the files in a web server. If directory browsing is disabled, an 'Access Forbidden' error message is displayed if the user attempts to access either a file or folder on the web server.

[41] One way to prevent GoogleBot from crawling content on a website is to use robots.txt to block access to files and directories on a server. 'Robots.txt' is a protocol used to request cooperating search robots not to access all or part of a website which is otherwise publicly accessible. Search engines comply with 'robots.txt' voluntarily and the OAIC has noted that most search engines comply with 'robots.txt', including Google, Bing and Yahoo.

Passwords and passphrases

Your entity should use passwords and passphrases to identify that users requesting access to your systems are authorised users. Passwords and passphrases should be complex enough so that others are not able to guess it, for example using a combination letters, numbers and symbols rather than actual words or common numbers.

- Is password or passphrase complexity enforced? For example, including uppercase characters, lowercase characters, punctuation, symbols, and/or numbers.
  - Are there mechanisms for changing them regularly?
  - Is reuse of passwords or passphrases blocked?
  - Is there a minimum length requirement? Is sharing of passwords or passphrases forbidden?
  - Are passwords or passphrases stored securely, such as in a 'hashed', 'salted'[42] or 'encrypted' format?
- Do accounts lock the user out after a specified number of failed logins?
  - Is a system administrator required to unlock accounts?
  - Do you suspend accounts that are unused or inactive for a period of time?
  - How quickly are accounts removed or suspended once someone leaves the entity?
- Are screen lock programs activated when computers are not in use? Do the screensavers properly blank out computer screens or fill them with moving images or patterns so that no personal information can be displayed when computers are not in use?
  - Do computers automatically lock if left inactive or unattended for periods of time?
  - Are users advised to lock their computers when they leave their desks, even for short periods?
- Are staff (including contractors) trained in the importance of strong passwords or passphrases and how to choose them?

Sometimes passwords are created using patterns that are known only to an entity and its staff (or part of its staff). Whilst each password is unique, there is a risk that a password may be inferred by someone who is aware of the pattern but is not authorised to access the file.

[42] 'Salting' is basically where an additional string of data, such as random numbers or text, is added to the password to make it less predictable and harder to attack, and 'hashing' is where passwords are processed through cryptographic algorithms that convert them into seemingly random characters. While passwords may be guessed through computational 'brute-force' attacks, this becomes very difficult when strong hash algorithms and passwords are used. Hashed passwords are therefore more secure to store than their clear-text passwords. The Australian Signals Directorate Information Security Manual (Control 1252, page 173) requires agencies to ensure usernames and passwords hashed with a strong hashing algorithm and uniquely salted.

Longer password patterns with many variations that are selected randomly rather than following a recognisable or known pattern are less likely to be guessed by unauthorised persons.

- Are passwords generated by patterns which are randomly selected and complex in terms of their length, character and order?

Collaboration

If you collaborate and share personal information with other entities while working on projects, you may continue to 'hold' personal information that is being used by the other collaborator. In these circumstances you must take reasonable steps to protect the information from unauthorised access while in their physical possession, including having effective controls in place to ensure that it is only accessed by authorised persons.

- How is the sharing of personal information managed to ensure access only by authorised persons?
  - How is access monitored?
  - Is the personal information shared using a secure method?
  - Is a platform that is managed, controlled or owned by another entity (such as a contract service provider), used to share the information? If so, what controls are in place to limit access?
  - Is the information encrypted and password protected? How are passwords managed and distributed to the user group?
  - Is there an access control policy in place which applies to everyone handling the personal information?
  - Are there policies and controls in place to prevent the unauthorised downloading, transferring or theft of bulk data shared with other entities, for example through the use of personal storage devices?

Audit logs, audit trails and monitoring access

Unauthorised access of personal information can be detected by reviewing a record of system activities, such as an audit log. Maintaining a chronological record of system activities (by both internal and external users) is often the best way for reviewing activity on a computer system to detect and investigate privacy incidents. Audit logs should also be named using a clear naming convention.

Audit trails are used to reconstruct and examine a sequence of activities on a system that lead to a specific event, such as a privacy incident.[43]

Access monitoring software that provides real time (or close to real time) dynamic review of access activity can also be useful for detecting unauthorised access to personal information.

[43] 'Audit log' and 'audit trail' are defined in the *Australian Signals Directorate Information Security Manual*, Glossary of Terms, p. 308

- What methods do you use to identify inappropriate access of files or databases containing personal information
  - Do you use audit logs and audit trails?
  - Is access by both internal and external persons monitored? Is there a method for identifying anomalous behaviour?
  - Are these measures mainly reactive (review of logs, responding to incidents) or do they also involve real time or close to real time monitoring of access activity? (also see 'Network security' section above).
- What points of access (such as access to devices, files, networks, databases, and websites) do you audit?
- Are audit logs reviewed on an on-going basis?
  - do you check/audit the activity of administrators?
- Does the audit log or audit trail indicate when an individual has:
  - accessed or viewed material
  - changed or destroyed material, or
  - unsuccessfully tried to access personal information?
- Does the audit log or audit trail enable actions to be linked to individuals, including both regular users and administrators?
- What procedures exist to address any issues, such as anomalous patterns of access, identified during a review of an audit log?
- How long are the audit logs kept for?
  - Are they part of a backup process?
- How are audit logs protected from tampering?
- Do logs or reports contain personal information and if so is it adequately protected?

Individuals accessing and correcting their own personal information

Under the Privacy Act, entities must, on request, give individuals access to the personal information held about them unless an exception applies.[44] Individuals are also able to request correction of the personal information held about them.[45]

- What processes do you have in place to assess requests from individuals to access or correct their personal information?

[44] See APP 12. Along with the right to request access under the Privacy Act, individuals have a right under the *Freedom of Information Act 1982* (Cth) (the FOI Act) to request access to information held by Australian Government agencies.

[45] See APP 13 - where an individual requests an APP entity to correct their personal information, APP 13.1 provides that the entity must take reasonable steps to correct the personal information it holds, to ensure it is accurate, up-to-date, complete, relevant, and not misleading, having regard to the purpose for which it is held'. Individuals also have rights under the FOI Act to have their personal information amended if it is out of date, misleading, incorrect or inaccurate.

- How do your staff identify customers/clients prior to disclosing their personal information online, by phone or in person?
- What measures do you take to ensure that these authentication processes do not result in collecting personal information that it is not reasonably necessary to collect?

Third party providers (including cloud computing)

Entities that outsource part or all of their personal information handling will need to consider whether they still 'hold' that personal information. If so, APP 11 will apply and you will need to take reasonable steps to comply with APP 11.

General issues

Relevant factors in deciding the steps that are reasonable in the circumstances include whether the third party is subject to the Privacy Act in its own right. Even if the third party is subject to the Privacy Act, if you hold the personal information, you still need to consider what steps are reasonable to protect the personal information. Steps may include influencing the third party's conduct.

Have you:

- conducted appropriate due diligence on the services to be provided (particularly data storage services)?
- considered the scope of the personal information handling services to be provided (for example, will the provider also backup your personal information holdings and if so what data will be captured)?
- considered what security controls and personal information handling measures you expect the third party supplier to use?
- included terms in the contract to deal with specific obligations about the handling of personal information and mechanisms to ensure the obligations are being fulfilled, such as regular reporting requirements
- for agencies, complied with s 95B of the Privacy Act which requires agencies to take contractual measures to ensure that a contracted service provider (as defined in the Privacy Act) does not do an act, or engage in a practice, that would breach an APP.[46]

[46] In particular, the agency must ensure that the contract does not authorise a contractor to do or engage in such an act or practice. An agency must also ensure the contract contains provisions to ensure that such an act or practice is not authorised by a subcontract.

Cloud computing

Cloud computing can range from data storage to the use of software programs, with data being stored and processed by the cloud service provider.[47] For instance, an entity can store data on remote servers operated by the cloud service provider rather than storing it on their own servers.

If you continue to 'hold' personal information when storing or using it in the cloud, reasonable steps may include robust management of the third party storing or handling your clients' personal information, including effective contractual clauses, verifying security claims of cloud service providers through inspections, and regular reporting and monitoring.

If you chose to adopt cloud computing you need to assess the security controls of the provider to ensure that you continue to comply with APP 11. However, other APPs may also apply in these circumstances, including APP 8 (where personal information is disclosed to an overseas recipient),[48] and APPs 12 and 13 (access and correction). These are discussed in more detail in the APP guidelines.

You should also consider whether your cloud service provider should be required to have similar controls to those you might apply to your own systems, such as governance arrangements and controls relating to software security, access security and network security set out in the sections above.

- Does the contract require the cloud service provider to put in place reasonable security steps that enable you to comply with your obligations under the APPs?
- From a security controls perspective, do you understand what controls you are responsible for and what your cloud service provider is responsible for?
- Are you able to verify the security controls of the cloud service provider to a sufficient level of detail, such as through independent testing and validation?
- Will those contractual obligations be reasonably easy to enforce from a costs and practicality perspective?
- Is the cloud service provider's information handling practices certified against information security standards (such as the ISO 27000 group)?[49]

[47] Cloud computing services have been defined as a way of sourcing and delivering ICT which enables convenient, on-demand network access to a shared pool of configurable computing resources (eg. networks, servers, storage, applications and services). The Australian Government has adopted the US Government's National Institute of Standards and Technology definition for cloud computing. For further information see the Australian Government's Cloud Computing Policy and supporting material which apply to the use of cloud services by Commonwealth entities, available on the Department of Finance's website at www.finance.gov.au/cloud/.

[48] You may also need to consider the data protection or privacy legislation in place where the data is stored by the cloud provider, as well as any other jurisdictions the cloud service provider may be subject to.

[49] In 2014, the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) also published ISO/IEC 27018:2014 which relates to the implementation of measures to protect personal information while it is being processed in the public cloud. The standard uses a definition of 'Personally Identifiable Information' adopted from ISO/IEC 29100:2011. If adopting this standard, entities

- Is the cloud service provider required to notify clients in the event of a data breach and does it have reasonable data breach response processes? In particular, are sufficient controls in place to properly investigate and respond to any suspected or actual breach to determine when and how it occurred, and what was taken?
- Does the cloud service provider enable secure transactions and encrypted storage?
- Have you considered encrypting the data yourself before transmission (rather than relying on the cloud service provider's encryption)?
- Have you considered who is able to decrypt data stored in the cloud?
- Does the cloud service provider intend to use your data for its own commercial purposes (separately or combined with other customers' data)? If so have you considered the security implications, including:
  - can you control the use of your data?
  - is the personal information de-identified before the provider uses it?
  - can you verify that the de-identified personal information cannot be re-identified?
- Does your cloud service provider subcontract to or use the resources of other parties to perform its services, and if so, how do they protect your data?
- Will your data be stored separately from the data of other customers of the cloud service provider; for example, on separate servers?
- Does the cloud service provider possess appropriate data recovery plans to deal with a natural disaster or system failure and prevent disclosure of your information?
- Is your data stored in a format you will be able to access or use if you need to retrieve it or amend it?
- Can the cloud service provider confirm whether it copies or otherwise replicates your information for its internal operational purposes (for example, if it moves your information between its IT assets), and what controls it has in place?
- Can the provider confirm that your information and any copies (including backups) have been destroyed at the conclusion of the contract? Can you retrieve the information?
- How easily can you contact a representative of the cloud service provider with privacy concerns?

must ensure that they apply the definitions of personal information and sensitive information in the Privacy Act. More information can be found in the 'Standards' section below.

Data breaches

In the event of a data breach, having a response plan that includes procedures and clear lines of authority can assist you to contain the breach and manage your response. Ensuring that staff (including contractors) are aware of the plan and understand the importance of reporting breaches is essential for the plan to be effective. The OAIC has published *Data breach notification: a guide to handling personal information security breaches*.

- Is there a data breach response plan and does it flow logically from any broader information security plan?
  - Is the plan regularly tested?
  - Does the plan include a strategy to assess and contain breaches?
  - Does the plan clearly identify those actions that are legislative or contractual requirements?
  - Are your staff educated about the plan and how to identify and respond to data breaches?
  - Does the plan enable staff to identify data breaches and require that breaches be reported?
  - Does the plan establish clear lines of command and indicate responsible officers?
  - Does the plan outline clearly when affected individuals should be notified of breaches?
  - Does the plan include a strategy to identify and address any weaknesses in data handling/data security that contributed to the breach?
- Are you required to notify affected individuals and the OAIC under law?[50]

Physical security

Physical security is an important part of ensuring that personal information is not inappropriately accessed. You need to consider what steps, if any, are necessary to ensure that physical copies of personal information are secure. Similarly, you should consider whether the workspace itself is designed to facilitate good privacy practices.

- What measures are used to control access to the workplace?
  - Are security and alarm systems used to control entry to the workplace?
  - Is it possible to identify staff movements from access logs?
- Are work areas with particular access to personal information (for example, human resources sections, complaints handling sections) physically segregated from other areas of business?

[50] Particular entities have mandatory data breach notification reporting obligations under s 75 of the PCEHR Act.

- Is there a record management system that identifies files and the location of responsible staff that contain personal information?
- Have privacy and security been considered when designing the workspace?
  - Are workstations positioned so that computer screens cannot be easily read by unauthorised third parties?
  - Do visitors have access to general workspaces or are there designated areas for them?
  - Are employees working on sensitive matters able to do so in a private/secure space, particularly in open plan workplaces?
  - Do employees have access to secure storage spaces near their workstations to secure documents temporarily?
- Is there a clean desk policy where personal information is being handled? Is it enforced?
- What provisions are made for securing physical files containing personal information?
  - How is the movement of physical files recorded?
  - Are storage and movement of files containing personal information audited or monitored?
  - On what basis is access to physical files granted?
  - If files are placed in lockable cabinets or similar, are these storage units kept locked? How is access to keys controlled?
- Are there procedures governing the transmission or transport of personal information to offsite work locations?

Destruction or de-identification of personal information

Where an entity holds personal information it no longer needs for a purpose that is permitted under the APPs, it must ensure that it takes reasonable steps to destroy or de-identify the personal information (APP 11.2) — in some cases, one or the other may be more appropriate. This obligation applies even where the entity does not physically possess the personal information, but has the right or power to deal with it.[51]

However, depending on the type of entity and the type of personal information involved, you may have specific obligations under law or a court/tribunal order to retain and/or destroy or de-identify personal information. Agencies also have specific retention obligations for personal information that forms part of a Commonwealth record.

- Do you have policies, procedures and resources in place to determine whether personal information you hold needs to be: retained under law or a court/tribunal order, destroyed or de-identified?

[51] See Chapter 11 of the APP guidelines for further guidance on the destruction or de-identification of personal information.

- Are your staff informed of document destruction procedures?

Destroying personal information — irretrievable destruction

Personal information is destroyed when it can no longer be retrieved. The steps that are reasonable for an entity to take to destroy personal information will depend on whether the personal information is held in hard copy or electronic form.

- Are your staff informed of document destruction procedures?
- Is destruction of personal information done in-house or outsourced?
    - If outsourced, what steps have you taken to ensure appropriate handling of the personal information?
- Has personal information contained in hard copy records that are disposed of through garbage or recycling collection been destroyed through a process such as pulping, burning, pulverising, disintegrating or shredding?
- Is hardware containing personal information in electronic form properly 'sanitised' to completely remove the stored personal information?
- Have steps been taken to verify the irretrievable destruction of personal stored by a third party on a third party's hardware, such as cloud storage, where the third party has been instructed by the organisation to irretrievably destroy the personal information, have steps been taken to verify that this has occurred?
- Are back-ups of personal information also destroyed? Are backups arranged in such a way that destruction of backups is possible? If not:
    - have steps been taken to rectify this issue in the future
    - has the backed-up personal information been put beyond use?
- How is compliance with data destruction procedures monitored and enforced?

Destroying personal information held in electronic form — putting beyond use

Where it is not possible for an entity to irretrievably destroy personal information held in electronic format, reasonable steps to destroy it would include putting the personal information 'beyond use'. For example, this could include where technical reasons may make it impossible to irretrievably destroy the personal information without also irretrievably destroying other information held with that personal information.

Personal information is 'beyond use' if you:

- are not able, and will not attempt, to use or disclose the personal information
- cannot give any other entity access to the personal information
- surround the personal information with appropriate technical, physical and organisational security. This should include, at a minimum, access controls including logs and audit trails, and
- commit to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible.

It is expected that only in very limited circumstances would it not be possible for an organisation to destroy personal information held in electronic format.

- Where it is not possible to irretrievably destroy personal information held in electronic format has the organisation taken steps to put the information 'beyond use'?

De-identifying personal information

De-identification of personal information may be more appropriate than destruction where the de-identified information could provide further value or utility to the entity or a third party, but you should consider whether de-identification is appropriate in the circumstances.

Personal information is de-identified under s 6 of the Privacy Act, 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.

- Do you have policies, practices and procedures in place to determine when it is appropriate to de-identify personal information?
  - How do you manage and mitigate the risk of re-identification?
  - Have steps been taken to verify the de-identification of personal stored by a third party (such as cloud storage)?

Standards

'Standards' are documents that set out requirements, specifications and procedures designed to ensure products, services and systems are safe, reliable and consistently perform in the way they are intended.[52] Standards can include guidelines, handbooks, manuals or policies and may be general or specific to particular industries or sectors, or practices.

Entities should consider using relevant international and Australian standards, policies, frameworks and guidance on information security. This includes any which are particular to their sector or industry (for example the *National eHealth Security and Access Framework*, which is relevant to the health sector).

Australian Government agencies must apply the Attorney-General's Department's *Protective Security Policy Framework* and the Australian Signals Directorate's *Australian Government Information Security Manual*. These documents articulate the Australian Government's requirements for protective security and standardise information security practices across government. They may also be used by other government agencies (including state and territory agencies) and the private sector as a model for better security practice.

[52] The term 'standards' is defined on the Standards Australia website at www.standards.org.au.

You may also want to consult the ISO/IEC 27000 series of information security management standards and the ISO/IEC 31000 of risk management standards published by both the International Organization for Standardization and the International Electrotechnical Commission, parts of which have been adopted by Standards Australia.[53] The 27000 series of standards provide recommendations on information security management, risks and controls. The 31000 series relates to standards for the design, implementation and maintenance of risk management processes. Compliance with standards can be tested internally or certified by a third party.

Adopting a standard is one way that you can gain some confidence regarding your security practices, but complying with a standard does not of itself mean that you have taken reasonable steps to protect personal information. It may be a reasonable step, but you may also need to take further action to meet your obligations under APP 11.

You may also seek to use certification of compliance with a standard as an assurance that you are protecting personal information. However, you will need to be aware of the scope of any certification, for example, whether it includes an assessment of the implementation of the relevant standard/s in practice; or the suitability of the risk profile underpinning the adoption of the standard/s. You will also need to aware of the extent to which you may rely on any certification of your processes or the processes of a party you are dealing with. Relying on the certification of your processes or the processes of a party you are dealing with may not of itself be considered 'reasonable steps' for the purposes of APP 11. You may need to take further action to meet your security obligations under APP 11.

In adopting any standard, you must make sure that you apply the definition of personal information and sensitive information from the Privacy Act, and not any other similar definitions that might by imported by or used in the standard.

- Have you considered standards particular to your industry or sector?
- If you have decided not to adopt a widely used standard, are the reasons for this decision clearly documented?
- Do you ensure that the standards you employ are the most current and appropriate?
- Is internal or external auditing undertaken to ensure compliance with relevant standards?
- If you have sought a certification of compliance with a relevant standard, did the scope of the certification include implementation; and the suitability of the risk profile underpinning the adoption of the standard?
- If auditing reveals areas of weakness or non-compliance with a standard, are these reported and addressed in a timely and complete manner?

[53] Further information regarding Australian and international standards is available from the Standards Australia website at www.standards.org.au and the International Organization for Standardization website at: www.iso.org.

Appendix A — Glossary of terms

Unless otherwise stated, terms used in this guide have the same meaning as in the Privacy Act. Some of these terms are explained in more detail in the APP guidelines.

Agency has the meaning set out in s 6(1) of the Privacy Act and includes a Commonwealth Minister, certain Australian Government agencies and the Norfolk Island administration.

APP entity means an agency or organisation and has the meaning set out in s 6(1) of the Privacy Act.

APPs means the Australian Privacy Principles which are set out in Schedule 1 of the Privacy Act.

CII means Commissioner initiated investigation, made under s 40(2) of the Privacy Act, where the Commissioner may, on his or her own initiative, investigate an act or practice that may be an interference with the privacy of an individual or a breach of APP 1. Investigations relating to acts or practices prior to 12 March 2014 use the term 'own motion investigation'.

Commonwealth record is defined in s 6(1) of the Privacy Act to have the same meaning as in s 3 of the *Archives Act 1983* (Cth).

CRB means credit reporting body and has the meaning set out in s 6 of the Privacy Act.

Credit provider has the meaning set out in s 6(1) of the Privacy Act.

CR Code means the *registered Privacy (Credit Reporting) Code 2014*, a mandatory code that binds credit providers and CRBs. The CR code supplements the provisions contained in Part IIIA of the Privacy Act and the *Privacy Regulation 2013*. A breach of the CR code is a breach of the Privacy Act.

Cth means Commonwealth.

Data breach means, for the purpose of this guide, when personal information held by an entity is lost or subjected to unauthorised access, use, interference, modification, disclosure, or other misuse.

Discloses is not defined in the Privacy Act and its meaning is discussed in the APP guidelines Chapter B: Key concepts, paragraphs B.57-B.63.

Entity means an agency, organisation or other person covered by the Privacy Act, including those covered by the APPs, Part IIIA and the *Tax File Number Guidelines 2011*.

Holds has the same meaning set out in s 6(1) of the Privacy Act (discussed in the APP guidelines Chapter B: Key concepts, paragraphs B.73-B.76) and as summarised on page 4 of this guide.

Information security means all measures used to protect any information generated by an entity or individual that is not intended to be made publicly available from compromise, loss of integrity or unavailability.

NPPs means the National Privacy Principles, which used to apply to organisations unless an exemption applied. The NPPs were replaced by the APPs on 12 March 2014.

OAIC means the Office of the Australian Information Commissioner.

Organisation has the meaning set out in s 6C of the Privacy Act and, in general, includes all businesses and non-government organisations with an annual turnover of more than $3 million, all health service providers regardless of turnover and a range of small businesses (see ss 6D and 6E of the Privacy Act).

Personal information has the meaning as set out in s 6(1) of the Privacy Act:

'Information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.'

Personal information security means keeping personal information secure from misuse, interference and loss, as well as unauthorised access, modification or disclosure.

PIA means privacy impact assessment and is discussed in the OAIC's Guide to undertaking privacy impact assessments.

Privacy Act means the *Privacy Act 1988* (Cth).

Sensitive information has the meaning as set out in s 6(1) of the Privacy Act and includes information or an opinion about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation, criminal record, health information and some aspects of genetic and biometric information.

TFN means a tax file number and has the meaning set out in Part VA of the *Income Tax Assessment Act 1936* (Cth).

TFN information means information that connects a TFN with the identity of a particular individual (for example, a database record that links a person's name and date of birth with the person's TFN).

Uses is not defined in the Privacy Act and its meaning is discussed in the APP guidelines Chapter B: Key concepts, paragraphs B.136-B.138.

Appendix B — Additional resources

OAIC resources

- The *Australian Privacy Principles guidelines*, which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters the OAIC may take into account when exercising functions and powers under the Privacy Act.
- The *Privacy Regulatory Action Policy*, which explains the OAIC's overall approach and priorities when using its privacy regulatory powers and making related public communications.
- *PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013* outlining how the OAIC will approach enforcement issues under the PCEHR Act.
- *Guide to undertaking privacy impact assessments* which provides assistance to entities on designing, conducting and acting on a privacy impact assessment.
- *Data breach notification: A guide to handling personal information security breaches*, which outlines steps that entities should consider in preparing for and responding to information security breaches, including notifying affected individuals.
- *Information Policy Agency Resource 1 — De-identification of Data and Information*, which provides general advice about de-identification, to assist agencies in balancing those objectives in information management.
- *Mobile Privacy: A Better Practice Guide for Mobile APP Developers*, which helps mobile device application (app) developers embed better privacy practices in their products and services, and help developers that are operating in the Australian market to comply with Australian privacy law and best practice.
- *Privacy Business Resource 4 — De-identification of data and Information*, which provides general advice about de-identification, to assist businesses and other organisations to protect privacy when using or sharing information assets containing personal information.
- *Privacy fact sheet 6 — The binding Tax File Number Guidelines 2011 and the protection of tax file number information* — which provides guidance related to the handling of TFNs, including the security obligations of TFN recipients.

Other resources

In addition, the following information security resources may be relevant to entities:

- CERT Australia is Australia's national computer emergency response team. CERT Australia is the single point of referral for cyber security incidents impacting upon Australian networks. CERT Australia provides advice and support on cyber threats and vulnerabilities to the owners and operators of Australia's critical infrastructure and other systems of national interest.

- *Control Objectives for Information and Related Technology* (COBIT) — COBIT 5 is the latest edition of ISACA's international framework for information technology (IT) management and IT governance.
- International standards published by the International Organization for Standardization (ISO) and Australian standards published by Standards Australia (see also the 'Standards' section in Part D of this guide), including the AS/NZS ISO/IEC 27000 series of information security management standards.
- *OECD Guidelines for the security of information systems and networks* is a framework of principles applicable to the security of information systems.
- The *National eHealth Security and Access Framework* (NESAF) is a comprehensive suite of documents regarding health security for the health industry and specific Australian health organisations. The NESAF aims to assist health organisations in meeting their security obligations.
- *StaySmartOnline* — this website provides guidance to businesses (and individuals) on measures they can take to protect personal and financial information online.
- *Managing the insider threat to your business - a personnel security handbook* - this handbook addresses the risk of the trusted insiders.

The following resources are particularly relevant to Australian Government agencies but are also useful for other organisations and government agencies:

- The *Australian Government Protective Security Policy Framework* (PSPF), which aims to enhance a stronger security culture and provide a common approach to the implementation of protective security by Australian Government agencies and which agency heads are required to apply. The PSPF may also be used by other government agencies (including state and territory agencies) as well as the private sector as a model for better security practice.
- *Information Security Management Guidelines — Risk management of outsourced ICT arrangements (including Cloud)* — the guidelines provide a consistent and structured approach to undertaking a risk assessment when considering outsourced ICT arrangements for Australian Government information.
- *Agency cyber security responsibilities when transacting online with the public* — which aims to assist agencies to understand and address their responsibility to minimise the risk of harm to the public when transacting online with the Australian Government.
- The Australian Signals Directorate (ASD) has a number of ICT security publications. including:
  - *Australian Government Information Security Manual*, which governs the security of government ICT systems
  - *Strategies to Mitigate Targeted Cyber Intrusions* a useful guide for both Government agencies and the private sector that contains a list of strategies to mitigate targeted cyber intrusions.

- The *National Identity Security Strategy* includes standards, best practices resources and tools (such as the Document Verification Service) to help agencies and other types of entities strengthen identification processes, secure identity records and documents and detect identity fraud. Resources are also available under the Strategy to help Australians protect their identity and respond to identity crime.
- The *National e-Authentication Framework*, developed by the Australian Department of Finance, assists Australian Government agencies and state jurisdictions in authenticating the identity of another party to a desired level of assurance or confidence.
- The Australian Government's policy on cloud computing for non-corporate agencies and supporting material on the Department of Finance's website.